CSC2125 Homework 2

Zi Han Zhao

1001103708

1 Claim: account model can reduce the average size of simple transfer transactions comparing to the UTXO model.

The claim is true. In UTXO model, if there is a large number of UTXO inputs and outputs, the corresponding locking and unlocking scripts take up a large space on chain. In account model, however, world state is stored in the node locally. When being faced with the multi-account transactions, only the signature and the transfer value are provided for each account.

In addition, in UTXO model, each input should be verified by visiting each source of the transfer value. The hash pointers pointing to each source also take up space on the chain. In account model, the balance of each account is stored and no need to store hash pointers to verify. It will save space as well.

2 Claim: comparing to the account model in Ethereum, the UTXO model can provide anonymous transactions if the user creates a new address for every transaction

The claim is true. In UTXO model, the user is encouraged to create each new address for each transaction. UTXO is a stateless model. If reusing a same address, all of the sources of the address amount are easily visited by hash pointers. Then the transaction history of the account address can be identified and learned. Different addresses from one single user are created so that it is hard to identify the addresses belong to the same user.

In account model in Ethereum, by contrast, the user is encouraged to reuse the same account address since each external account owns its multiple contract accounts. Keeping a single account is easier to manage and organize. It decreases the degree of privacy since all of the transactions are related with a single account.

3 Why Ethereum introduces a GAS limit for the block? What if we remove the GAS limit and put back the traditional block limit of 1MB like Bitcoin?

When executing a function in smart contract, sometimes attackers can find a way to run into an infinite loop and claim funds from another contract address. Gas limit is introduced to prevent the unlimited gas consumption. During execution, the gas is consumed gradually by each EVM operation until reaching gas limit. The infinite loop execution is stopped and the function call is reverted and the account only pays for the value of the pre-set gas limit.

If replacing gas limit with block limit, it cannot solve unlimited gas consumption during execution. Block limit only defines the size of executed smart contract. EVM is Turing completed machine. The size of a infinite loop could be small enough in a block, which still causes the unlimited gas consumption.

4 Ethereum sets up a different GAS amount for different EVM operations. Why?

The computation cost of each EVM operation is different. E.g., ADD operation is cheaper than memory access operations. If the gas amount is set the same for each operation, no miners execute cost-heavy smart contract if given the same gas fee. It leads some contract transaction being never picked by miners.